

United States District Court

DISTRICT OF ARIZONA

In the Matter of the Search of

CASE NUMBER: 21-5307MB

3650 W. South Butte Road
San Tan Valley, Arizona 85142

SEARCH AND SEIZURE WARRANT

TO: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

See Attachment A-1, incorporated by reference

The affidavit in support of this Search Warrant is herein incorporated by reference or attached.

The person or property to be searched, described above, is believed to conceal:

See Attachment B-1, incorporated by reference

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 12/20/21

Date (Not to Exceed 10 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 3103a (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of _____.

Date and Time Issued Dec. 6, 2021 @ 11:53am

Deborah M. Fine
Judge's Signature

City and state:

Phoenix, Arizona

Deborah M. Fine, United States Magistrate Judge

Printed Name and Title

ATTACHMENT A-1

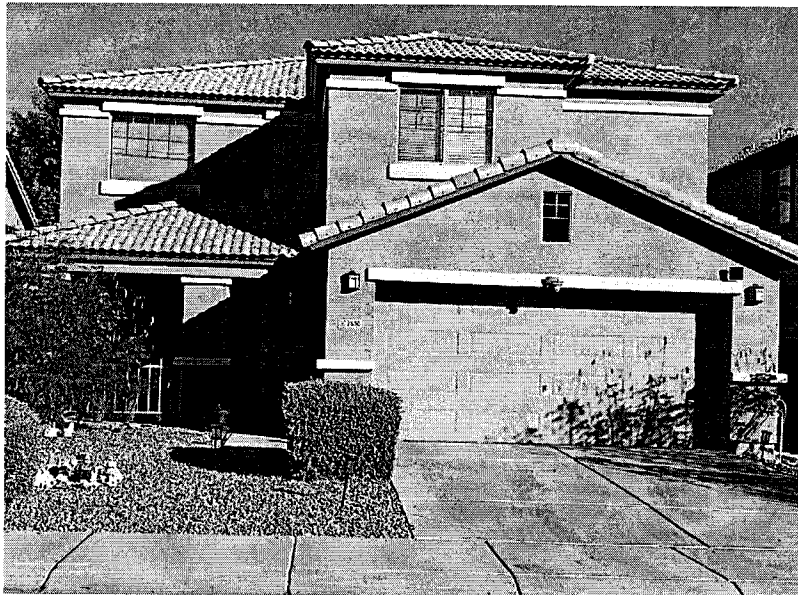
DESCRIPTION OF PREMISES TO BE SEARCHED:

The entire premises and curtilage located at 3650 W. South Butte Road, San Tan Valley, Arizona 85142-6474. This is a tan two story home with light tan trim and tiled roof. The residence has a concrete driveway leading to a tan two car garage door on the east side of the residence. The front door is set back from the street on a covered porch towards the center of the residence. Affixed on the west side of the garage, attached to the stucco of the residence, is a plaque with the numbers 3650. The residence is located on the north side of the street, four houses to the west of the intersection of W. South Butte Road and N. Cactus Way.

The property is identified in the records of the Pinal County Assessor's Office as Parcel# 509-95-1480.

Two photographs of the residence are on the following page:

*3650 W. South Butte Road
San Tan Valley, Arizona 85142*



Front of Residence



Front Door of Residence

ATTACHMENT B-1
PROPERTY TO BE SEIZED

Agents are authorized to search for evidence of violations of Title 18, United States Code, Section 1546(a) (False Statement on Immigration Document, and Use, Attempted Use or Possession of an Alien Registration Card Unlawfully Obtained); Title 18, United States Code, Section 1425(a) (Attempted Unlawful Procurement of Citizenship or Naturalization); and Title 18, United States Code, Section 1015(a) (False Statement Relating to Naturalization, Citizenship or Alien Registry) as further described in the Affidavit. This evidence, which may be related to date range of at least 1971 to the present, and supports the criminal offenses outlined in the Affidavit, includes:

1. Any and all documents, records, and physical objects related to NAJAR's prior association with, involvement and membership in, or assistance to the military in Peru, including: correspondence, recordings, photographs, service records, paystubs, receipts, contacts, videotapes, memorabilia, paraphernalia, uniforms, patches, decorations, medals, insignia, or weapons;
2. Any and all documents, records, and physical objects related to NAJAR's prior involvement in any criminal acts in Peru including but not limited to the extrajudicial killings, torture and forced disappearances of the residents of Cayara in May 1988, corruption, and drug trafficking including: media reports, charging or arrest documents, court records, correspondence, photographs, service records, paystubs, receipts contacts, videotapes, memorabilia, paraphernalia, uniforms, patches, decorations, medals, insignia, or weapons;
3. Any and all documents, records, and physical objects, including identification cards and identifying documents, related to NAJAR's presence in the United States and travel to and from the United States;
4. Any and all documents, records, and objects related to NAJAR's immigration to (and obtaining permanent residence in, and applying for naturalization with) the United States, immigration to and from other countries, the Immigration and Naturalization Service, the Department of Homeland Security and any component therein, the U.S. Department of

State, and any federal or foreign government issued identification documents, including any and all applications and forms, passports, visas, and domestic or foreign identification cards, plane tickets and/or itineraries;

5. Any and all records, documents, and correspondence with third parties pertaining to NAJAR's applications for an immigrant visa, permanent resident status, and naturalization, in which NAJAR discusses questions on immigration documents and applications;

6. Records indicating occupancy, residency, rental or ownership of the search location, including utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, and keys.

7. Electronic devices and equipment, including cellular telephones, computers, tablets, disks, thumb drives, and any media storage device, GPS devices and their memory, used to generate, transfer, count, record or store the information described in this attachment.

8. For any electronic device or storage medium described in the preceding paragraph whose seizure otherwise is authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "ELECTRONIC DEVICE"):

a. evidence of who used, owned, or controlled the ELECTRONIC DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the ELECTRONIC DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the ELECTRONIC DEVICE of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the ELECTRONIC DEVICE;

f. evidence of the times the ELECTRONIC DEVICE was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the ELECTRONIC DEVICE;

h. documentation and manuals that may be necessary to access the ELECTRONIC DEVICE or to conduct a forensic examination of the ELECTRONIC DEVICE;

i. records of or information about Internet Protocol addresses used by the ELECTRONIC DEVICE;

j. records of or information about the ELECTRONIC DEVICE 's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

k. contextual information necessary to understand the evidence described in this attachment.

9. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

10. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical

form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

11. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

PROCEDURES TO BE FOLLOWED FOR CERTAIN MATERIALS

12. During the search for relevant evidence (as described above), if agents find any document that appears to contain or reflect communications with an attorney, including Peruvian attorney Dr. Arturo Visurraga Agüero, or any document otherwise appearing that it may be protected by the attorney-client privilege or attorney work-product doctrine, the agents immediately will cease reviewing the document and will place it in a box clearly marked as containing potentially privileged materials. The government will arrange to have any such materials reviewed by government personnel not otherwise involved in this case (the "Filter Team") to determine whether, in fact, the materials are protected from disclosure or whether they may be released to the case team, including, if necessary, in redacted form. Similarly, if agents or other government personnel find potentially protected materials when reviewing the contents of electronic evidence seized during the search, the agents immediately will cease reviewing the item of electronic evidence in question, provide it to the Filter Team, and direct the Filter Team to search and review the item for potentially protected materials to determine whether, in fact, the materials are protected from disclosure or whether they may be released to the case team, including, if necessary, in redacted form.